UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/818,699	03/27/2001	Doug L. Rollins	MPATENT.163A	9926

20995 7590 02/13/2006

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 02/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/818,699	ROLLINS, DOUG L.	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 November 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) *2-4* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 5-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *July 6, 2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the RCE dated November 21, 2005.

Claims 1 and 5-9 are pending.

Response to Arguments

2. Applicant's arguments with respect to claims 1 and 5-9 have been considered but are moot in view of the new ground(s) of rejection. Applicant's arguments focus on the combination of features introduced by the amendment with elements that already existed in the claims. The new material is rendered obvious by Simmons et al. (2001/0039659), Pardikar et al. (2003/0046366), Schneier (Applied cryptography), Prihoda et al. (6,789,195) and Eldridge (6,094,721).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 5 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Simmons et al. (2001/0039659) in view of Pardikar et al. (2003/0046366) and further in view of Schneier (Applied cryptography).

a) As to claim 1, Simmons discloses a system and method for enabling a user to request and download selected files from provider sites (Abstract) comprising: storing independently of information from the network server a public and a private encryption key in a client computer system (Fig. 2, element 56; page 3, paragraph 0041, i.e. locally generated encryption key); sending a request for a data file from client to server (page 1, paragraph 0006, i.e. home user requests media file from server); and in response to the request, automatically retrieve the key from client computer system, encrypting the data file with the key automatically and without user intervention and sending the encrypted data file to the client computer system (page 1, paragraph 0016; page 3, paragraph 0041 and page 4, paragraph 0046).

Simmons does not explicitly disclose checking a file attribute to determine that the file is to be encrypted with the public encryption key.

Pardikar discloses a system and method for providing transparent and automatic file access comprising checking a file attribute to determine that the file is to be encrypted (page 6, paragraph 0061).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of checking a file attribute to determine that the file is to be encrypted in the system of Simmons as Pardikar teaches so as to provide security of those files that are determined to be protected.

Simmons discloses encryption keys however he does not explicitly disclose public and private encryption key where the data file is encrypted with public key.

Schneier discloses public key algorithm where often the encryption key is called the public key and the decryption key is called private key (pages 4-5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of public key algorithm in the system of Simmons and Pardikar as Schneier teaches so as to efficiently encrypt data files.

b) As to claims 5 and 8, Simmons discloses a system and method for enabling a user to request and download selected files from provider sites (Abstract) comprising: storing independently of information from the network server a public and a private encryption key in a client computer system (Fig. 2, element 56; page 3, paragraph 0041, i.e. locally generated encryption key); sending a request for a data file from client to server (page 1, paragraph 0006, i.e. home user requests media file from server); and in response to the request, automatically retrieve the key from client computer system, encrypting the data file with the key automatically and without user intervention and sending the encrypted data file to the client computer system (page 1, paragraph 0016; page 3, paragraph 0041 and page 4, paragraph 0046) and storing the encrypted data file on a storage medium in the client computer system (Fig. 8, element 210).

Simmons does not explicitly disclose checking a file attribute to determine that the file is to be encrypted with the public encryption key.

Pardikar discloses a system and method for providing transparent and automatic file access comprising checking a file attribute to determine that the file is to be encrypted (page 6, paragraph 0061).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of checking a file attribute to determine that the file is to be encrypted in the system of Simmons as Pardikar teaches so as to provide security of those files that are determined to be protected.

Simmons discloses encryption keys however he does not explicitly disclose public and private encryption key where the data file is encrypted with public key.

Schneier discloses public key algorithm where often the encryption key is called the public key and the decryption key is called private key (pages 4-5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of public key algorithm in the system of Simmons and Pardikar as Schneier teaches so as to efficiently encrypt data files.

5. Claims 6 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Simmons et al. (2001/0039659) in view of Pardikar et al. (2003/0046366) in view of Schneier (Applied cryptography) and further in view of Prihoda et al. (6,789,195).

As to method of claim 6 and data storage medium of claim 9, Simmons, Pardikar and Schneier do not explicitly disclose an attribute (associated with the file) indicating the file is unencrypted when stored on the network server.

Prihoda discloses the data are encrypted while being transmitted between the client and server, the data then exist in unencrypted form at the central point and are generally stored in unencrypted form in a central database (col. 1, lines 22-27).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of attribute to indicate file is unencrypted when stored on the server as Prihoda teaches in the system of Simmons, Pardikar and Schneier so as to provide adequate protection to data.

6. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Simmons et al. (2001/0039659) in view of Pardikar et al. (2003/0046366) in view of Schneier (Applied cryptography) and further in view of Eldridge et al. (6,094,721).

Simmons, Pardikar and Schneier do not explicitly disclose the public and private key are based on a password.

Elridge discloses a method and apparatus for updating the password status of one of more servers in a client/server environment comprising public and corresponding private key derived from password (col. 5, lines 33-46).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of generating public and private key from a password as Elridge teaches in the system of Simmons, Pardikar and Schneier so as to secure password access.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
2/1/06

GUY LAMARRE
PRIMARY EXAMINER